Claims:

1. A method for detecting unauthorized intrusion in a network system, comprising the steps of:

receiving packet level activity information from the network;

sorting port specific activity information from the received packet level activity information;

monitoring the port specific activity information; and

executing at least one of a blocking action or a tracking action based upon the monitored port specific activity information.

2. The method according to claim 1, wherein the step of monitoring includes:

identifying presence of at least one activity from the port specific activity information;

assigning a binary representation (1 = present, 0=absent) to the at least one identified activity; and

generating an assessment based upon the binary rating.

3. The method according to claim 2, wherein the step of generating an assessment includes associating the binary rating with an assessment based upon predetermined behavioral criteria.

4. The method according to claim 3, wherein the step of generating an assessment includes mapping the assessment on at least one two-dimensional grid.

5. The method according to claim 4, wherein the step of mapping occurs dynamically and in real-time.

6. The method according to claim 2, wherein the step of generating an assessment includes generating a profile of user based upon the monitored port specific activity information.

7. The method according to claim 2, wherein the step of generating an assessment is carried out utilizing a back propagation network.

8. The method according to claim 7 wherein the back propagation network includes psychological assessment information.

9. The method according to claim 2, wherein the assessment is one of high deception/high expertise, high deception/low expertise, low deception/high expertise and low deception/low expertise.

10. The method according to claim 1, wherein the blocking action includes sending a blocking command to a firewall for blocking further network access.

11. The method according to claim 1, wherein the tracking action includes storing activity information in a tracking module.

12. A system for preventing unauthorized intrusion in a network system, comprising:

a traffic sorter;

an activity monitor operatively coupled to the traffic sorter;

an inter-port fusion module operatively coupled to the activity monitor; and

an outcome director operatively coupled to the inter-port fusion monitor.

13. The system according to claim 12, wherein the activity monitor includes at least one dedicated port monitor.

14. The system according to claim 13, wherein, the at least one dedicated port monitor includes a packet level analysis module, an activity translator module and an assessment module.

15. The system according to claim 14, wherein the assessment module includes a back propagation network.

16. The system according to claim 15, wherein the back propagation network includes psychological assessment information.

17. The system according to claim 14, wherein the traffic sorter receives packet level activity information from the network and sorts the port specific activity information from the network.

18. The system according to claim 14, wherein the activity monitor monitors the port specific activity information.

19. The system according to claim 14, wherein the activity translator module assigns a binary rating based upon presence (1) or absence (0) of at least one activity detected by the packet level analysis module.

20. The system according to claim 19, wherein the assessment module generates an assessment result based upon the binary rating.

21. The system according to claim 19, wherein the assessment module maps the assessment result utilizing at least one of a two dimensional grid or X dimensional grid for optional real-time viewing of a user's intent.

22. The system according to claim 20, wherein an outcome director initiates at least one of a blocking command or a tracking command based upon the assessment result.

23. The system according to claim 22, wherein the blocking command is directed to a system firewall.

24. The system according to claim 23 in which a blocking command results in the storage of all session data indicating all user activity and intent until such time as access is terminated.

25. The system according to claim 22, wherein the tracking command is directed to a tracking module.

26. The system according to claim 24, wherein the tracking module includes a tracking database for storing activity information that may be used to provide evidence of an intruder's harmful intent activities and at least one intent assessment during a session.

27. The system according to claim 26, wherein the tracking database includes neural network assessment and associated information for the intruder that is at least one of tracked or blocked.

28. The system according to claim 27, wherein the tracking database includes a comparison module for comparing the neural network assessment and associated information against a second assessment based upon a second network intrusion.

29. The system according to claim 28, wherein at least one of a blocking or tracking action is executed based upon an output from the comparison module.

30. A system for detecting unauthorized intrusion in a network system, comprising:

sorting means for sorting port specific activity from incoming packet level activity;

monitoring means operatively coupled to the sorting means for monitoring the sorted port specific activity; and

assessing means operatively coupled to the monitoring means for generating an assessment.

31. A computer program product, comprising:

a computer usable medium having computer readable code embodied therein for preventing unauthorized intrusion into a computer network, the computer program product comprising:

computer readable program code configured to cause the computer to sort port specific activity information from packet level activity information received by the computer network;

computer readable program code configured to cause the computer to monitor port specific activity information; and

computer readable program code configured to cause the computer to execute at least one of a blocking action or a tracking action based upon the monitored port specific activity information.